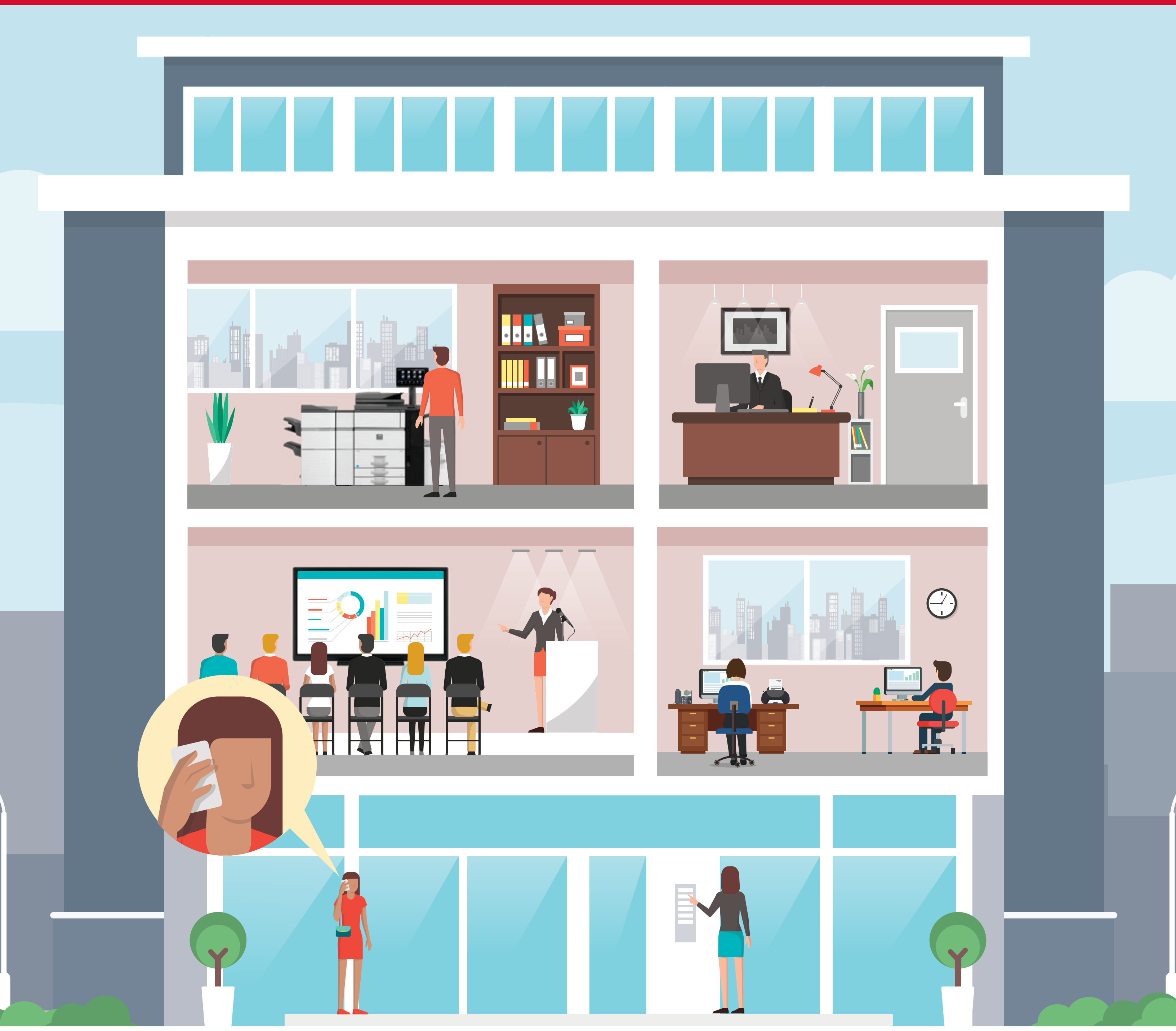
How Secure is your Office



Multifunction Printers

- Unclaimed documents left at the device can end up in the wrong hands
- Outdated and unsecured MFPs can serve as a “secret” backdoor into your network
- Hackers can steal printer logs with sensitive information or cause damage to a device
- Files sent through a wireless connection to be printed can be intercepted

of businesses lose their data through printer security breaches.[1]

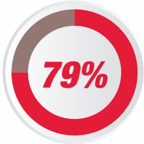
IoT Devices

- All internet connected devices represent a possible entryway into your network
- IoT devices lacking the latest operating system updates are more vulnerable
- Dead or unsupported apps can serve as a potential gateway to your network
- Smartphones and tablets containing sensitive company data can be lost or stolen

of device manufacturers did not feel confident their devices had adequate security precautions in place.[2]

Computers

- Outdated firewall, antivirus, and operating systems widen your gap of vulnerability
- Weak network traffic restrictions can lead to infections from corrupt emails and websites
- Malicious software can take control of your computer and files not backed up can be lost



of companies could have prevented a breach with a software patch or configuration change.[3]

Employees

- Global spending on security awareness training for employees is one of the fastest growing categories in cybersecurity
- It only takes one click on the wrong email or website for a hacker to have access to your network
- Downloading unverified software can infect your system

of successful hacks and data breaches stem from phishing scams.[4]

Sources: Small Business Trends (1), IoT For All: Current State of IoT Cybersecurity (2), Voke Research Market Snapshot Report (3), Cybersecurity Ventures (4)

SHARP®